Monitorowanie i bezpieczeństwo sieci komputerowych : ćwiczenia laboratoryjne / Krzysztof Nowicki, Tadeus Uhl. – Szczecin, 2016

Spis treści

Wstęp **7**

Ćwiczenie 1: Monitorowanie sieci - WireShark, PackETH, Netstat **9**
1. Wprowadzenie 9
2. Konfiguracja sprzętu laboratoryjnego 12
3. Wykorzystywane narzędzia do analizy sieci 15
3.1. Wireshark - opis narzędzia 15
3.2. PackETH - opis narzędzia 29
3.3. Netstat - opis narzędzia 34
4. Zadania 37

Ćwiczenie 2: Monitorowanie usług sieciowych oraz zasobów systemowych - Nagios **39**
1. Wprowadzenie 39
2. Konfiguracja sprzętu laboratoryjnego 43
3. Monitorowanie dostępności hostów 44
4. Monitorowanie usług 47
5. NRPE - konfiguracja demona i wtyczki check NRPE 51

Ćwiczenie 3: Podsłuchiwanie - sniffery **53**
1. Wprowadzenie 53
2. Konfiguracja sprzętu laboratoryjnego 55
3. Przebieg zajęć w laboratorium 62
3.1. Przechwytywanie hasła 62
3.2. Przechwytywanie obrazów 63
3.3. Przekierowywanie ruchu w sieci 63
3.4. Przechwytywanie haseł z https 64
3.5. Zalewanie tablicy CAM 65

Ćwiczenie 4: Wykrywanie podsłuchu - antysniffery **71**
1. Wprowadzenie 71
2. Schemat stanowiska laboratoryjnego oraz wykorzystywane systemy operacyjne i programy 73
3. Metody sniffowania oraz sposoby bronienia się 75
3.1. Tryb promiscuous 75
3.2. MAC flooding 81
3.3. Wykrywanie ataku ARP spoofing 83
3.4. Funkcja port-security w przełączniku CISCO 85

Ćwiczenie 5: Ataki na mechanizmy sieci VLAN **89**
1. Wprowadzenie 89
2. Ataki na sieci VLAN 99
2.1. VLAN Hopping 99
2.2. Switch Spoofing 99
2.3. Double Tagging 99
2.4. Obrona przed atakami 99
3. Przygotowanie i konfiguracja środowiska 101
4. Scenariusze laboratoryjne 103
Zadanie 1: Atak typu Double Tagging 103
Zadanie 2: Atak typu ARP poisoning 103

Ćwiczenie 6: Ataki na mechanizmy STP **105**
1. Wprowadzenie 105
2. Ataki na STP 110
2.1. Podszywanie się pod Roota 110
2.2. Zalewanie urządzenia ramkami BPDU 113
2.3. Obrona przed atakami 117
3. Przygotowanie środowiska 118
4. Scenariusze ćwiczeń 119
Zadanie 1: Konfiguracja sieci z STP 119
Zadanie 2: Atak na STP - rozsyłanie pakietów BPDU configuration 119
Zadanie 3: Atak na STP - rozsyłanie ramek BPDU topology change notification 121

Ćwiczenie 7: System kontroli dostępu na portach IEEE 802.1x **123**
1. Wprowadzenie 123
2. Konfiguracja środowiska 133
3. Scenariusze ćwiczeń 139
Zadanie 1: Ustawienie portów przełącznika w tryb uwierzytelniania 802.1x 140
Zadanie 2: Uwierzytelnianie w systemach Windows i Linux 140
Zadanie 3: Ataki na system zabezpieczony protokołem 802.1x 141

Literatura **145**

Spis rysunków **146**

Spis tabel **147**

oprac. BPK